Пустые улицы, одиночный лай собак, маски на лицах, антисептики, и тревожная новостная повестка.

КИБЕРБЕЗОПАСНОСТЬ ВО ВРЕМЯ БОРЬБЫ С ПАНДЕМИЕЙ COVID-19

ROOT LEVEL RESOURCES

Коронавирус заставил людей всего мира оставаться дома и переводить свою работу на удаленный режим. В первые дни удаленной работы компании столкнулись с проблемой построения технологических процессов. Вид такой работы не соответствует уровню кибербезопасности, который есть в офисе, в результате чего может ослабнуть компьютерная безопасность этих компаний, что с большой вероятностью приведет к увеличению успешности атак на системы процессинга, SWIFT, банкоматные сети и платежные шлюзы. К росту количества успешных атак на системы процессинга, SWIFT, сети банкоматов и платежные шлюзы могут привести два фактора:

1

Неправильное подключение компьютеров через VPN к внутренним сервисам, при которой домашний компьютер сотрудника окажется за пределами периметровых средств защиты.

2

Сотрудники не смогут из дома оперативно и скоординированно реагировать на поступающие угрозы.

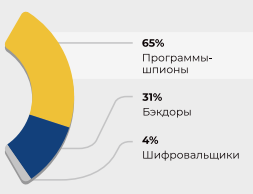
Еще одна проблема — рост нагрузки и нехватка серверных мощностей.

Такая ситуация создает крайне высокий риск самых различных угроз – от заражения инфраструктуры уже известными сетевыми вирусами до хакерских атак. В группе риска — сотрудники финансовых учреждений, телекомоператоров и IT-компаний, а целью кибератак станет не только кража денег или персональных данных, но и проникновение в корпоративную инфраструктуру через личный компьютер жертвы.

Фишинговые письма во время пандемии коронавируса

В период с 13.02.2020 по 01.04.2020 специалисты CERT-GIB проанализировали сотни фишинговых писем, замаскированных под информационные и коммерческие рассылки о COVID-19. Письма были написаны от имени международных организаций (ВОЗ, ЮНИСЕФ), а также крупных российских и международных компаний. Рассылки были направлены как в коммерческий, так и в государственный секторы России и СНГ. Эти сообщения были перехвачены системой Threat Detection System (TDS).

Перехваченные фишинговые письма содержали во вложении различные типы шпионского ПО:



Программы-шпионы способны собирать данные о системе и зараженном компьютере, загружать и запускать файлы, делать скриншоты, записывать нажатие клавиш на клавиатуре, а также могут похищать данные пользователей, логины, пароли из браузеров, почтовых клиентов, а также данные банковских карт.

Наиболее востребованные трояны для шпионского ПО

Несмотря на то, что процент фишинговых писем, паразитирующих на теме COVID-19, невысок и составил за исследуемый период порядка 5% во всем вредоносном трафике, злоумышленники на хакерских форумах стремятся использовать панические настроения, чтобы поднять свои продажи вредоносных программ.

Так, с февраля на андеграундном форуме продается замаскированное под интерактивную карту распространения COVID-19 ПО. Основным путем заражения является обычная фишинговая рассылка, способная обходить защиту Gmail. После заражения пользователю открывается карта с актуальными данными ВОЗ и Университета Джона Хопкинса, а параллельно загружается любая "полезная нагрузка", например, вредоносная программа для кражи данных. В целом, экспертами было зафиксировано более 500 объявлений на андеграундных площадках со скидками и промокодами на период пандемии на услуги DDoD, спам-рассылок и т.д.

Кроме того, специалистами компании Group-IB было обнаружено появление фальшивых уведомлений об уплате штрафа за нарушение самоизоляции, а именно:

В апреле 2020 года, по Краснодарскому краю проводились соответствующие рассылки через смс или мессенджеры, при этом в сообщениях были указаны фамилия, имя и отчество получателя. Получателям приходили уведомления с требованием оплатить штраф в 4 тыс. руб.[1] по несуществующему постановлению Федеральной службы исполнения наказаний (ФСИН), рассказали в компании.

В этих уведомлениях говорилось, что штраф якобы нужно было заплатить в течение суток переводом на номер абонента в Краснодарском крае. Тех, кто звонил по указанному номеру, переводили на номер, который якобы принадлежит справочной службе МВД РФ.

Специалисты отметили, что мошенники использовали подобную схему и в прошлом году: тогда они рассылали уведомления о «штрафах» за посещение порносайтов.

Стоит отметить, что Краснодарский край стал лидером по количеству протоколов, составленных за нарушение карантина (введен в регионе с 31 марта). В суды региона поступило более 1,3 тыс. дел об административных правонарушениях по ст. 6.3 КоАП РФ (нарушение законодательства в области обеспечения санитарно-эпидемиологического благополучия), более 1 тыс. из них уже рассмотрены.

Совсем немного уступает Республика Татарстан, где ограничения на передвижение граждан введены 30 марта. Там по ст. 6.3 КоАП РФ было выписано более 800 протоколов.

Кроме того, стремительно растет количество мошеннических сообщений и сайтов, которые используют тему коронавируса, чтобы украсть у пользователей деньги или личные данные.

Фальшивые электронные пропуска

Коронавирус существенно изменил режим жизни граждан, что в свою очередь привело к появлению аферистов, предлагающих услуги по оформлению электронных пропусков.

Специалисты отметили, что первые попытки интернет-мошенничеств на фоне борьбы с пандемией COVID-19 были зафиксированы еще в конце марта, еще до введения первых ограничений на передвижение и системы электронных пропусков. Еще при начале самоизоляции, по данным Group-IB, эксперты отдела расследований компании обратили внимание на сомнительные предложения через один популярный мессенджер о покупке пропусков для свободного передвижения по Москве, Санкт-Петербургу и Краснодару. Для получения поддельного пропуска интернет-аферисты просили прислать им паспортные данные и, если требовался пропуск на автомобиль, его госномер. Обязательным условием была стопроцентная предоплата услуг, которая составляла от 2,5 тыс. до 6 тыс. руб. в зависимости от типа пропуска и сайта. После перечисления требуемой суммы на кредитную карту переписка с клиентом сразу же прекращалась, а сам он заносился в черный список, чтобы не мешать общению с другими кандидатами на получение заветного пропуска.

Тем не менее оперативники уголовного смогли вычислить двух администраторов интернет-ресурса — ими оказались молодые люди 19 и 23 лет. 21 апреля оба были задержаны. Управление организации дознания ГУ МВД по Москве уже возбудило уголовное дело по статье о мошенничестве (ч. 1 ст. 159 УК РФ). Не исключено, что позднее речь может пойти о переквалификации действий задержанных по более «тяжелой» части статьи УК РФ.

По данным Департамента инновационной защиты бренда и интеллектуальной собственности Group-IB, уже обнаружено 126 мошеннических ресурсов, торгующих цифровыми пропусками:

35 групп и аккаунтов в соцсетях — **25 сайтов** — **66 Telegram-каналов**

Продажа аккаунтов ZOOM

Одним из самых популярных инструментов образования во время карантина стали онлайн-конференции, организованные в программе Zoom. Компания Zoom Video Communications, производящая одноименный сервис для видеосвязи, была основана в 2011 году. Суточная аудитория приложения в мире в марте 2020 года по сравнению с декабрем 2019 года выросла в 20 раз, до 200 миллионов человек.

В свою очередь, специалисты Group-IB обнаружили объявления о продаже учетных записей пользователей Zoom на трех андеграундных площадках. Общее количество уникальных записей, выставленных на продажу на данный момент, составляет 4 153, среди которых 31 аккаунт принадлежит пользователям с почтовым адресом в домене .ru. Проверить, действительно ли эти учетные данные принадлежат пользователям Zoom, не представляется возможным.

Ранее Блумберг сообщил о двух исках, поданных против Zoom из-за предполагаемого разглашения конфиденциальной информации пользователей. В частности, в иске, поданном частным лицом в суд калифорнийского города Сан-Хосе, утверждалось, что компания собирает информацию о пользователях без соответствующего уведомления во время установки или открытия приложения Zoom, а затем передает данные третьим сторонам, в том числе компании Facebook.

МИД ФРГ строго ограничило использование сотрудниками сервиса на служебных устройствах из-за возможных угроз безопасности, сообщало издание Handelsblatt со ссылкой на внутренний документ министерства. А по данным Financial Time, сенат США не рекомендует к использованию Zoom для проведения конференций сенаторов из-за опасений, связанных с безопасностью данных.

ROOT LEVEL RESOURCES

Говорят, после пандемии COVID-19 мир уже не будет прежним. Несмотря на постепенное ослабление карантина во всем мире, значительное количество офисных работников продолжает работать из дома. Это ставит под угрозу безопасность организаций, поскольку контролировать производительность работников и следить за безопасностью их устройств в таких условиях гораздо сложнее.

В таких ситуациях важным остается соблюдение правил кибербезопасности. Прежде всего на каждом устройстве, которое используется для работы и имеет доступ к конфиденциальным данным должно быть установлено программное обеспечение для защиты от угроз — начиная от фишинговых ссылок в электронных письмах или социальных сетях до вредоносных программ.

Кроме использования решений для кибербезопасности рекомендуют придерживаться основных правил кибергигиены. Они помогут поддерживать безопасность устройств и своевременно выявлять подозрительную деятельность злоумышленников даже после возвращения к прежней жизни.

1 – Москвичам за нарушение режима самоизоляции грозит штраф до 5 тыс. руб. Кроме того, нарушители режима самоизоляции могут быть приговорены к более крупным штрафам — от 15 тыс. до 300 тыс. руб. — по федеральному Кодексу об административных правонарушениях (нарушение законодательства в области обеспечения санитарно-эпидемиологического благополучия населения).